

JCS64 U.S. PRO  
09/504070

Applicants : Masayuki TERADA et al.

Serial No. : To Be Assigned

Filed : Herewith

For : ORIGINAL DATA CIRCULATION METHOD, SYSTEM,  
APPARATUS, AND COMPUTER READABLE MEDIUM

CLAIM TO CONVENTION PRIORITY UNDER 35 U.S.C. 119

A claim to the Convention Priority Date of each of the following Japanese Patent Applications is being made at the time this United States application is being filed.

In order to complete the claim to Convention Priority Dates under 35 U.S.C. 119, a certified copy of each of these Japanese applications is enclosed herewith.

**KENYON & KENYON**

One Broadway  
New York, N.Y. 10004  
(212) 425-7200  
Dated: February 14, 2000  
EXPRESS MAIL EL039790667US

PATENT OFFICE  
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy  
of the following application as filed with this office.

Date of Application: September 1, 1999

Application Number: Japanese Patent Application  
No. 11-247457

Applicant(s): NIPPON TELEGRAPH AND TELEPHONE  
CORPORATION

January 14, 2000

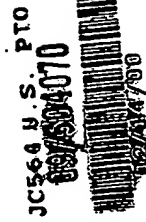
Commissioner,  
Patent Office

Takahiko Kondo (Seal)

Certificate No. 11-3094228

*Express Mail EL03979066 705.*

PATENT OFFICE  
JAPANESE GOVERNMENT



This is to certify that the annexed is a true copy  
of the following application as filed with this office.

Date of Application: February 17, 1999

Application Number: Japanese Patent Application  
No. 11-039080

Applicant(s): NIPPON TELEGRAPH AND TELEPHONE  
CORPORATION

January 14, 2000

Commissioner,  
Patent Office

Takahiko Kondo (Seal)

Certificate No.11-3094216

*Express Mail E203979066705*

日 本 国 特 許 庁

PATENT OFFICE  
JAPANESE GOVERNMENT

JC564 U. S. PTO  
09/504070  
02/14/00

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application:

1999年 2月17日

出 願 番 号  
Application Number:

平成11年特許願第039080号

出 願 人  
Applicant (s):

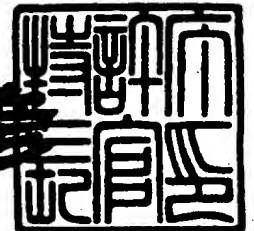
日本電信電話株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2000年 1月14日

特許庁長官  
Commissioner,  
Patent Office

近 藤 隆 彦



【書類名】 特許願

【整理番号】 NTTH106951

【提出日】 平成11年 2月17日

【あて先】 特許庁長官 伊佐山 建志 殿

【国際特許分類】 G06F 13/38

【発明者】

    【住所又は居所】 東京都新宿区西新宿三丁目 19 番 2 号 日本電信電話株式会社内

    【氏名】 寺田 雅之

【特許出願人】

    【識別番号】 000004226

    【氏名又は名称】 日本電信電話株式会社

【代理人】

    【識別番号】 100070150

    【弁理士】

    【氏名又は名称】 伊東 忠彦

【手数料の表示】

    【予納台帳番号】 002989

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

    【物件名】 図面 1

    【物件名】 要約書 1

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ蓄積方法及びシステム及びデータ蓄積プログラムを格納した記憶媒体

【特許請求の範囲】

【請求項 1】 価値を有する電子的な情報の蓄積を行うデータ蓄積方法において、

電子的な情報の発行者装置により該電子的な情報に署名した第 1 の情報を付与し、

前記発行者装置により前記電子的な情報と対応するマニフェストの第 2 の情報を生成して、前記第 1 の情報に付与し、

電子的な情報利用装置において、前記第 1 の情報と前記第 2 の情報を用いて電子的な情報の発行者装置の同一性を判定し、電子的な情報の複製を防止することを特徴とするデータ蓄積方法。

【請求項 2】 電子的な情報の発行を厳重に管理されたサーバの発行する検証鍵を取得し、

前記情報利用装置において、前記検証鍵からセッション情報を生成し、

前記セッション情報の正当性を判定する請求項 1 記載のデータ蓄積方法。

【請求項 3】 前記第 2 の情報を耐タンパ性の装置に格納し、前記発行者装置の同一性を判定し、前記電子的な情報の複製を防止する請求項 1 記載のデータ蓄積方法。

【請求項 4】 価値を有する電子的な情報の蓄積を行うデータ蓄積システムであって、

電子的な情報に署名した第 1 の情報を付与し、該電子的な情報と対応するマニフェストの第 2 の情報を生成して、前記第 1 の情報に付与する発行者装置と、

前記第 1 の情報と前記第 2 の情報を用いて電子的な情報の発行者装置の同一性を判定し、電子的な情報の複製を防止する利用者装置とを有することを特徴とするデータ蓄積システム。

【請求項 5】 前記利用者装置は、

電子的な情報の発行を厳重に管理されたサーバの発行する検証鍵を取得する手

段を有し、

前記検証鍵からセッション情報を生成する手段と、

前記セッション情報の正当性を判定する手段を有する改札装置を更に有する請求項 4 記載のデータ蓄積システム。

【請求項 6】 前記利用者装置は、

前記第 2 の情報を耐タンパ性の装置に格納し、前記発行者装置の同一性を判定する手段を含む請求項 4 記載のデータ蓄積システム。

【請求項 7】 価値を有する電子的な情報の蓄積を行うデータ蓄積システムであって、

生成者を特定可能な情報である署名を電子情報に付与する第 1 の署名手段と、

前記署名が付与された情報の格納及び抽出を行うための第 1 の格納手段と、

前記電子的な情報と 1 対 1 に対応するマニフェストの格納及び抽出を行うための第 2 の格納手段と、

前記電子的な情報に付与された署名の生成者である署名者と該電子的な情報に対応するマニフェストを格納しようとする格納者とが同一であることを検証するための第 1 の認証手段と、

前記署名手段により署名が付与された署名付き情報を格納する際に、該署名付き情報を前記第 1 の格納手段に格納すると共に、該署名の署名者と該署名付き情報に対応するマニフェストの格納者とが同一であることが前記第 1 の認証手段により検証された時のみ、該マニフェストを前記第 2 の格納手段に格納する第 1 の制御手段とを有する利用者装置を有することを特徴とするデータ蓄積システム。

【請求項 8】 前記利用者装置の前記第 2 の格納手段及び前記第 1 の認証手段は、耐タンパ性を有する請求項 7 記載のデータ蓄積システム。

【請求項 9】 前記第 1 の認証手段は、

前記第 1 の格納手段に格納された前記署名が付与された情報の有効性を、該情報と対応するマニフェストが前記第 2 の格納手段に格納されているか否かにより検証し、該マニフェストが該第 2 の格納手段に格納されていた時のみ該情報が有効であるとし、該マニフェストが該第 2 の格納手段に格納されていなかったときには、該情報を無効とする手段を含む請求項 7 記載のデータ蓄積システム。

【請求項 10】 前記電子的な情報の署名者が信用する署名者を指定する信任対象の 1 つまたは複数の集合からなる信任情報を生成する信任情報生成手段と

、  
マニフェストに、署名を付与するための第 2 の署名手段と、

マニフェストの格納及び抽出を行う第 3 の格納手段と、

マニフェストの署名者が信任対象または、信任対象がさらに信用する署名者に含まれること、及び該信任情報の署名者と、前記情報の署名者とが同一であることを検討する第 2 の認証手段と、

ある電子的な情報に対応するマニフェストを前記第 2 の格納手段から前記第 3 の格納手段に移動させる際に、該第 2 の格納手段から該マニフェストを抽出し、前記第 2 の署名手段により該マニフェストに署名を付与し、該第 2 の格納手段から該マニフェストを削除し、該マニフェストの署名者を該電子的な情報の署名者が信用することを前記第 2 の認証手段により検証し、検証に成功した時のみ前記第 3 の格納手段に該マニフェストを格納する第 2 の制御手段とを有する発行者装置を有する請求項 7 記載のデータ蓄積システム。

【請求項 11】 前記発行者装置の前記第 3 の格納手段、第 2 の署名手段、前記第 2 の認証手段が耐タンパ性を有する請求項 10 記載のデータ蓄積システム

。   
【請求項 12】 システム内で一意性を持つセッション情報を生成するセッション情報生成手段と、

前記セッション情報の格納及び抽出を行うための第 4 の格納手段とを具備する改札装置を更に有し、

前記改札装置は、

ある電子的な情報に対応するマニフェストを前記利用者装置の前記第 2 の格納手段から前記発行者装置の前記第 3 の格納手段に移動させる際に、前記セッション情報生成手段によりセッション情報を生成し、前記第 4 の格納手段に該セッション情報を格納し、

前記利用者装置は、

前記第 2 の格納手段から前記マニフェストを抽出し、



前記発行者装置は、

前記第2の署名手段により該マニフェストと該セッション情報の組に署名を付与し、該第2の格納手段から該マニフェストを削除し、該組の署名者を該電子的な情報の署名者が信用することを前記第2の認証手段により認証し、

前記改札装置は、

前記第2の認証手段において認証が成功し、かつ、該組に含まれるセッション情報が、前記第4の格納手段に格納されていたときのみ、該第4の格納手段から該セッション情報を削除し、

前記発行者装置は、

前記第3の格納手段に前記マニフェストを格納する請求項7及び10記載のデータ蓄積システム。

【請求項13】 価値を有する電子的な情報の蓄積を行うデータ蓄積システムであって、

生成者を特定可能な情報である署名を電子情報に付与する第1の署名手段と、

前記署名が付与された情報の格納及び抽出を行うための第1の格納手段と、

前記電子的な情報と1対1に対応するマニフェストの格納及び抽出を行うための第2の格納手段と、

前記電子的な情報に付与された署名の生成者である署名者と該電子的な情報に対応するマニフェストを格納しようとする格納者とが同一であることを検証するための第1の認証手段と、

前記署名手段により署名が付与された署名付き情報を格納する際に、該署名付き情報を前記第1の格納手段に格納すると共に、該署名の署名者と該署名付き情報に対応するマニフェストの格納者とが同一であることが前記第1の認証手段により検証された時のみ、該マニフェストを前記第2の格納手段に格納する第1の制御手段とを有する利用者装置と、

前記電子的な情報の署名者が信用する署名者を指定する信任対象の1つまたは複数の集合からなる信任情報を生成する信任情報生成手段と、

マニフェストに、署名を付与するための第2の署名手段と、

マニフェストの格納及び抽出を行う第3の格納手段と、

マニフェストの署名者が信任対象または、信任対象がさらに信用する署名者に含まれること、及び該信任情報の署名者と、前記情報の署名者とが同一であることを検討する第2の認証手段と、

ある電子的な情報に対応するマニフェストを前記第2の格納手段から前記第3の格納手段に移動させる際に、該第2の格納手段から該マニフェストを抽出し、前記第2の署名手段により該マニフェストに署名を付与し、該第2の格納手段から該マニフェストを削除し、該マニフェストの署名者を該電子的な情報の署名者が信用することを前記第2の認証手段により検証し、検証に成功した時のみ前記第3の格納手段に該マニフェストを格納する第2の制御手段とを有する発行者装置とを有することを特徴とするデータ蓄積システム。

【請求項14】 価値を有する電子的な情報の蓄積を行うデータ蓄積システムであって、

生成者を特定可能な情報である署名を電子情報に付与する第1の署名手段と、  
前記署名が付与された情報の格納及び抽出を行うための第1の格納手段と、  
前記電子的な情報と1対1に対応するマニフェストの格納及び抽出を行うための第2の格納手段と、

前記電子的な情報に付与された署名の生成者である署名者と該電子的な情報に対応するマニフェストを格納しようとする格納者とが同一であることを検証するための第1の認証手段と、

前記署名手段により署名が付与された署名付き情報を格納する際に、該署名付き情報を前記第1の格納手段に格納すると共に、該署名の署名者と該署名付き情報に対応するマニフェストの格納者とが同一であることが前記第1の認証手段により検証された時のみ、該マニフェストを前記第2の格納手段に格納する第1の制御手段とを有する利用者装置と、

前記電子的な情報の署名者が信用する署名者を指定する信任対象の1つまたは複数の集合からなる信任情報を生成する信任情報生成手段と、

マニフェストに、署名を付与するための第2の署名手段と、

マニフェストの格納及び抽出を行う第3の格納手段と、

マニフェストの署名者が信任対象または、信任対象がさらに信用する署名者に

含まれること、及び該信任情報の署名者と、前記情報の署名者とが同一であることを検討する第2の認証手段と、

ある電子的な情報に対応するマニフェストを前記第2の格納手段から前記第3の格納手段に移動させる際に、該第2の格納手段から該マニフェストを抽出し、前記第2の署名手段により該マニフェストに署名を付与し、該第2の格納手段から該マニフェストを削除し、該マニフェストの署名者を該電子的な情報の署名者が信用することを前記第2の認証手段により検証し、検証に成功した時のみ前記第3の格納手段に該マニフェストを格納する第2の制御手段とを有する発行者装置と、

システム内で一意性を持つセッション情報を生成するセッション情報生成手段と、

前記セッション情報の格納及び抽出を行うための第4の格納手段とを具備する改札装置を具備し、

前記利用者装置は、

前記第2の格納手段から前記マニフェストを抽出し、

前記発行者装置は、

前記第2の署名手段により該マニフェストと該セッション情報の組に署名を付与し、該第2の格納手段から該マニフェストを削除し、該組の署名者を該電子的な情報の署名者が信用することを前記第2の認証手段により認証し、

前記改札装置は、

前記第2の認証手段において認証が成功し、かつ、該組に含まれるセッション情報が、前記第4の格納手段に格納されていたときのみ、該第4の格納手段から該セッション情報を削除し、

前記発行者装置は、

前記第3の格納手段に前記マニフェストを格納することを特徴とするデータ蓄積システム。

【請求項15】 価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおける発行者装置に搭載されるデータ蓄積プログラムを格納した記憶媒体であって、

電子的な情報に署名した第1の情報に付与し、該電子的な情報と対応するマニフェストの第2の情報を生成して、前記第1の情報に付与するプロセスを有することを特徴とするデータ蓄積プログラムを格納した記憶媒体。

【請求項16】 価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおける利用者装置に搭載されるデータ蓄積プログラムを格納した記憶媒体であって、

前記第1の情報と前記第2の情報をを用いて電子的な情報の発行者装置の同一性を判定し、電子的な情報の複製を防止するプロセスを有することを特徴とするデータ蓄積プログラムを格納した記憶媒体。

【請求項17】 電子的な情報の発行を厳重に管理されたサーバの発行する検証鍵を取得するプロセスと、

前記検証鍵からセッション情報を生成するプロセスと、

前記セッション情報の正当性を判定するプロセスを含む請求項16記載のデータ蓄積プログラムを格納した記憶媒体。

【請求項18】 価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおける利用者装置に搭載されるデータ蓄積プログラムを格納した記憶媒体であって、

生成者を特定可能な情報である署名を電子情報に付与する第1の署名プロセスと、

前記署名が付与された情報を第1の記憶手段に格納すると共に、抽出を行うための第1の格納プロセスと、

前記電子的な情報と1対1に対応するマニフェストを第2の記憶手段に格納すると共に、抽出を行うための第2の格納プロセスと、

前記電子的な情報に付与された署名の生成者である署名者と該電子的な情報に対応するマニフェストを格納しようとする格納者とが同一であることを検証するための第1の認証プロセスとを有することを特徴とするデータ蓄積プログラムを格納した記憶媒体。

【請求項19】 前記第1の認証プロセスは、

前記第1の記憶手段に格納された前記署名が付与された情報の有効性を、該情

報と対応するマニフェストが前記第2の記憶手段に格納されているか否かにより検証し、該マニフェストが該第2の記憶手段に格納されていたときのみ該情報が有効であるとし、該マニフェストが該第2の記憶手段に格納されていなかったときには、該情報を無効とするプロセスを含む請求項18記載のデータ蓄積プログラムを格納した記憶媒体。

【請求項20】 価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおける発行者装置に搭載されるデータ蓄積プログラムを格納した記憶媒体であって、

前記電子的な情報の署名者が信用する署名者を指定する信任対象の1つまたは複数の集合からなる信任情報を生成する信任情報生成プロセスと、

マニフェストに、署名を付与するための第2の署名プロセスと、

マニフェストを第3の記憶手段に格納すると共に、抽出を行う第3の格納プロセスと、

マニフェストの署名者が信任対象または、信任対象がさらに信用する署名者に含まれること、及び該信任情報の署名者と、前記情報の署名者とが同一であることを検討する第2の認証プロセスとを有することを特徴とするデータ蓄積プログラムを格納した記憶媒体。

【請求項21】 価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおける改札装置に搭載されるデータ蓄積プログラムを格納した記憶媒体であって、

システム内で一意性を持つセッション情報を生成するセッション情報生成プロセスと、

前記セッション情報を第4の記憶手段に格納すると共に抽出を行うための第4の格納プロセスとを有することを特徴とするデータ蓄積プログラムを格納した記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、データ蓄積方法及びシステム及びデータ蓄積プログラムを格納した

記憶媒体に係り、特に、電子チケットなどの権利を表象するデータやデジタル著作物など、有効な複製数を一定以下に保つことが必要とされるデータについて、蓄積や配送のための手段を提供するためのデータ蓄積方法及びシステム及びデータ蓄積プログラムを格納した記憶媒体に関する。

【0002】

【従来の技術】

権利を表象したデータや著作物などは、配布者などの意図する数を越えて同時に複製が存在することを防止することが求められる。即ち、配布したデータが利用者などにより複製され、それらが多重に利用されることを防ぐ必要がある。

従来は、以下で示すような技術によりそのような多重利用を防止している。

【0003】

第1の方法として、権利を表象するデータについて、権利の提供者などにより、当該データの使用履歴を保持しておき、権利の行使時に、当該データが既に使用されていないかどうかを検証する。もし、既に使用されていれば、当該データが表象する権利の行使を拒否する。

第2の方法として、データ自身を耐タンパ装置に格納し、当該データを当該耐タンパ装置以外からは参照できないようにする。権利の行使時には、当該データを該耐タンパ装置より抹消する。

【0004】

【発明が解決しようとする課題】

しかしながら、上記従来の第1の方法では、耐タンパ装置などの特別な装置を必要としていないが、データを転々流通させる際に問題が生じる。即ち、当該技術では、行使時の事後検出しか行えないため、流通過程では、当該データの有効性は判定できないという問題がある。

【0005】

従来の第2の方法では、耐タンパ装置を用いることにより、データの唯一性を保証することができる。また、（特願平6-503913）や、（特開平9-511350）などで述べられている方式などを併用し、暗号によって保護された安全な通信路を介して耐タンパ装置を結合し、当該通信路を介してデータの授受

を行うことにより、当該データの流通を、複製を事前に防止しながら行うことを可能とする。しかしながら、当該技術は、耐タンパ装置の中にデータを格納する必要があるため、以下の2点が問題となる。

【0006】

まず、データの記述そのものを見ることができなくなるため、記述の正当性の検証など、複製に関する有効性以外の検証も全て当該耐タンパ装置に委ねなければならないという制約が生じる。

また、データの格納部のみならず、データの取扱に必要な処理も全て耐タンパ装置が負わなければならないため、耐タンパ装置に対して記憶容量や処理速度に大きな要求が発生する。特に、現時点で耐タンパ装置として一般的なICカードでは、処理速度や記憶容量に不足が生じる。

【0007】

本発明は、上記の点に鑑みなされたもので、データの有効な複製数を一定以下に保つことを保証しつつ、記述の正当性の検証を含む複製に関する有効性以外の検証をすべて耐タンパ装置に委ねることなく、処理速度や記憶容量等の処理負荷を低減させるデータ蓄積方法及びシステム及びデータ蓄積プログラムを格納した記憶媒体を提供することを目的とする。

【0008】

【課題を解決するための手段】

図1は、本発明の原理を説明するための図である。

本発明（請求項1）は、価値を有する電子的な情報の蓄積を行うデータ蓄積方法において、

電子的な情報の発行者装置により該電子的な情報に署名した第1の情報を付与し（ステップ1）、

発行者装置により電子的な情報と対応するマニフェストの第2の情報を生成して、第1の情報に付与し（ステップ2）、

電子的な利用者装置において、第1の情報と第2の情報を用いて電子的な情報の発行者装置の同一性を判定し（ステップ3）、電子的な情報の複製を防止する。

【 0 0 0 9 】

本発明（請求項 2）は、電子的な情報の発行を厳重に管理されたサーバの発行する検証鍵を取得し、

利用者装置において、検証鍵からセッション情報を生成し、  
セッション情報の正当性を判定する。

本発明（請求項 3）は、第 2 の情報を耐タンパ性の装置に格納し、発行者装置の同一性を判定し、電子的な情報の複製を防止する。

【 0 0 1 0 】

図 2 は、本発明の原理構成図である。

本発明（請求項 4）は、価値を有する電子的な情報の蓄積を行うデータ蓄積システムであって、

電子的な情報に署名した第 1 の情報を付与し、該電子的な情報と対応するマニフェストの第 2 の情報を生成して、第 1 の情報に付与する発行者装置 1 と、

第 1 の情報と第 2 の情報を用いて電子的な情報の発行者装置 1 の同一性を判定し、電子的な情報の複製を防止する利用者装置 2 とを有する。

【 0 0 1 1 】

本発明（請求項 5）は、上記のシステムにおいて、

利用者装置 2 は、電子的な情報の発行を厳重に管理されたサーバの発行する検証鍵を取得する手段を有し、

検証鍵からセッション情報を生成する手段と、

セッション情報の正当性を判定する手段を有する改札装置を更に有する。

【 0 0 1 2 】

本発明（請求項 6）は、利用者装置 2 において、

第 2 の情報を耐タンパ性の装置に格納し、発行者装置の同一性を判定する手段を含む。

本発明（請求項 7）は、生成者を特定可能な情報である署名を電子情報に付与する第 1 の署名手段と、署名が付与された情報の格納及び抽出を行うための第 1 の格納手段と、

電子的な情報と 1 対 1 に対応するマニフェストの格納及び抽出を行うための第



2の格納手段と、

電子的な情報に付与された署名の生成者である署名者と該電子的な情報に対応するマニフェストを格納しようとする格納者とが同一であることを検証するための第1の認証手段と、

署名手段により署名が付与された署名付き情報を格納する際に、該署名付き情報を第1の格納手段に格納すると共に、該署名の署名者と該署名付き情報に対応するマニフェストの格納者とが同一であることが第1の認証手段により検証された時のみ、該マニフェストを第2の格納手段に格納する第1の制御手段とを有する利用者装置を有する。

【0013】

本発明（請求項8）は、利用者装置の第2の格納手段及び第1の認証手段において、耐タンパ性を有する。

本発明（請求項9）は、第1の認証手段において、

第1の格納手段に格納された署名が付与された情報の有効性を、該情報と対応するマニフェストが第2の格納手段に格納されているか否かにより検証し、該マニフェストが該第2の格納手段に格納されていたときのみ該情報が有効であるとし、該マニフェストが該第2の格納手段に格納されていなかったときには、該情報を無効とする手段を含む。

【0014】

本発明（請求項10）は、電子的な情報の署名者が信用する署名者を指定する信任対象の1つまたは複数の集合からなる信任情報を生成する信任情報生成手段と、

マニフェストに、署名を付与するための第2の署名手段と、

マニフェストの格納及び抽出を行う第3の格納手段と、

マニフェストの署名者が信任対象または、信任対象がさらに信用する署名者に含まれること、及び該信任情報の署名者と、情報の署名者とが同一であることを検討する第2の認証手段と、

ある電子的な情報に対応するマニフェストを第2の格納手段から第3の格納手段に移動させる際に、該第2の格納手段から該マニフェストを抽出し、第2の署

名手段により該マニフェストに署名を付与し、該第2の格納手段から該マニフェストを削除し、該マニフェストの署名者を該電子的な情報の署名者が信用することを第2の認証手段により検証し、検証に成功した時のみ第3の格納手段に該マニフェストを格納する第2の制御手段とを有する発行者装置を有する。

【0015】

本発明（請求項11）は、発行者装置の第3の格納手段、第2の署名手段、第2の認証手段が耐タンパ性を有する。

本発明（請求項12）は、システム内で一意性を持つセッション情報を生成するセッション情報生成手段と、

セッション情報の格納及び抽出を行うための第4の格納手段とを具備する改札装置を更に有し、

改札装置において、

ある電子的な情報に対応するマニフェストを利用者装置の第2の格納手段から発行者装置の第3の格納手段に移動させる際に、セッション情報生成手段によりセッション情報を生成し、第4の格納手段に該セッション情報を格納し、

利用者装置において、

第2の格納手段からマニフェストを抽出し、

発行者装置において、

第2の署名手段により該マニフェストと該セッション情報の組に署名を付与し、該第2の格納手段から該マニフェストを削除し、該組の署名者を該電子的な情報の署名者が信用することを第2の認証手段により認証し、

改札装置において、

第2の認証手段において認証が成功し、かつ、該組に含まれるセッション情報が、第4の格納手段に格納されていた時のみ、該第4の格納手段から該セッション情報を削除し、

発行者装置において、

第3の格納手段にマニフェストを格納する。

【0016】

本発明（請求項13）は、価値を有する電子的な情報の蓄積を行うデータ蓄積

システムであって、

生成者を特定可能な情報である署名を電子情報に付与する第1の署名手段と、

署名が付与された情報の格納及び抽出を行うための第1の格納手段と、

電子的な情報と1対1に対応するマニフェストの格納及び抽出を行うための第2の格納手段と、

電子的な情報に付与された署名の生成者である署名者と該電子的な情報に対応するマニフェストを格納しようとする格納者とが同一であることを検証するための第1の認証手段と、

署名手段により署名が付与された署名付き情報を格納する際に、該署名付き情報を第1の格納手段に格納すると共に、該署名の署名者と該署名付き情報に対応するマニフェストの格納者とが同一であることが第1の認証手段により検証された時のみ、該マニフェストを第2の格納手段に格納する第1の制御手段とを有する利用者装置と、

電子的な情報の署名者が信用する署名者を指定する信任対象の1つまたは複数の集合からなる信任情報を生成する信任情報生成手段と、

マニフェストに、署名を付与するための第2の署名手段と、

マニフェストの格納及び抽出を行う第3の格納手段と、

マニフェストの署名者が信任対象または、信任対象がさらに信用する署名者に含まれること、及び該信任情報の署名者と、情報の署名者とが同一であることを検討する第2の認証手段と、

ある電子的な情報に対応するマニフェストを第2の格納手段から第3の格納手段に移動させる際に、該第2の格納手段から該マニフェストを抽出し、第2の署名手段により該マニフェストに署名を付与し、該第2の格納手段から該マニフェストを削除し、該マニフェストの署名者を該電子的な情報の署名者が信用することを第2の認証手段により検証し、検証に成功した時のみ第3の格納手段に該マニフェストを格納する第2の制御手段とを有する発行者装置とを有する。

【0017】

本発明（請求項14）は、価値を有する電子的な情報の蓄積を行うデータ蓄積システムであって、

生成者を特定可能な情報である署名を電子情報に付与する第1の署名手段と、  
署名が付与された情報の格納及び抽出を行うための第1の格納手段と、

電子的な情報と1対1に対応するマニフェストの格納及び抽出を行うための第2の格納手段と、

電子的な情報に付与された署名の生成者である署名者と該電子的な情報に対応するマニフェストを格納しようとする格納者とが同一であることを検証するための第1の認証手段と、

署名手段により署名が付与された署名付き情報を格納する際に、該署名付き情報を第1の格納手段に格納すると共に、該署名の署名者と該署名付き情報に対応するマニフェストの格納者とが同一であることが第1の認証手段により検証された時のみ、該マニフェストを第2の格納手段に格納する第1の制御手段とを有する利用者装置と、

電子的な情報の署名者が信用する署名者を指定する信任対象の1つまたは複数の集合からなる信任情報を生成する信任情報生成手段と、

マニフェストに、署名を付与するための第2の署名手段と、

マニフェストの格納及び抽出を行う第3の格納手段と、

マニフェストの署名者が信任対象または、信任対象がさらに信用する署名者に含まれること、及び該信任情報の署名者と、情報の署名者とが同一であることを検討する第2の認証手段と、

ある電子的な情報に対応するマニフェストを第2の格納手段から第3の格納手段に移動させる際に、該第2の格納手段から該マニフェストを抽出し、第2の署名手段により該マニフェストに署名を付与し、該第2の格納手段から該マニフェストを削除し、該マニフェストの署名者を該電子的な情報の署名者が信用することを第2の認証手段により検証し、検証に成功した時のみ第3の格納手段に該マニフェストを格納する第2の制御手段とを有する発行者装置と、

システム内で一意性を持つセッション情報を生成するセッション情報生成手段と、

セッション情報の格納及び抽出を行うための第4の格納手段とを具備する改札装置を具備し、

利用者装置において、

第 2 の格納手段からマニフェストを抽出し、

発行者装置において、

第 2 の署名手段により該マニフェストと該セッション情報の組に署名を付与し、  
該第 2 の格納手段から該マニフェストを削除し、該組の署名者を該電子的な情報の署名者が信用することを第 2 の認証手段により認証し、

改札装置において、

第 2 の認証手段において認証が成功し、かつ、該組に含まれるセッション情報が、第 4 の格納手段に格納されていたときのみ、該第 4 の格納手段から該セッション情報を削除し、

発行者装置において、

第 3 の格納手段にマニフェストを格納する。

【 0 0 1 8 】

本発明（請求項 1 5）は、価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおける発行者装置に搭載されるデータ蓄積プログラムを格納した記憶媒体であって、

電子的な情報に署名した第 1 の情報を付与し、該電子的な情報と対応するマニフェストの第 2 の情報を生成して、第 1 の情報に付与するプロセスを有する。

【 0 0 1 9 】

本発明（請求項 1 6）は、価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおける利用者装置に搭載されるデータ蓄積プログラムを格納した記憶媒体であって、

第 1 の情報と第 2 の情報を用いて電子的な情報の発行者装置の同一性を判定し、電子的な情報の複製を防止するプロセスを有する。

【 0 0 2 0 】

本発明（請求項 1 7）は、電子的な情報の発行を厳重に管理されたサーバの発行する検証鍵を取得するプロセスと、

検証鍵からセッション情報を生成するプロセスと、

セッション情報の正当性を判定するプロセスを含む。

本発明（請求項 18）は、価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおける利用者装置に搭載されるデータ蓄積プログラムを格納した記憶媒体であって、

生成者を特定可能な情報である署名を電子情報に付与する第 1 の署名プロセスと、

署名が付与された情報を第 1 の記憶手段に格納すると共に、抽出を行うための第 1 の格納プロセスと、

電子的な情報と 1 対 1 に対応するマニフェストを第 2 の記憶手段に格納すると共に、抽出を行うための第 2 の格納プロセスと、

電子的な情報に付与された署名の生成者である署名者と該電子的な情報に対応するマニフェストを格納しようとする格納者とが同一であることを検証するための第 1 の認証プロセスとを有する。

【0021】

本発明（請求項 19）は、第 1 の認証プロセスは、

第 1 の記憶手段に格納された署名が付与された情報の有効性を、該情報と対応するマニフェストが第 2 の記憶手段に格納されているか否かにより検証し、該マニフェストが該第 2 の記憶手段に格納されていたときのみ該情報が有効であるとし、該マニフェストが該第 2 の記憶手段に格納されていなかったときには、該情報を無効とするプロセスを含む。

【0022】

本発明（請求項 20）は、価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおける発行者装置に搭載されるデータ蓄積プログラムを格納した記憶媒体であって、

電子的な情報の署名者が信用する署名者を指定する信任対象の 1 つまたは複数の集合からなる信任情報を生成する信任情報生成プロセスと、

マニフェストに、署名を付与するための第 2 の署名プロセスと、

マニフェストを第 3 の記憶手段に格納すると共に、抽出を行う第 3 の格納プロセスと、

マニフェストの署名者が信任対象または、信任対象がさらに信用する署名者に

含まれること、及び該信任情報の署名者と、情報の署名者とが同一であることを検討する第2の認証プロセスとを有する。

【0023】

本発明（請求項21）は、価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおける改札装置に搭載されるデータ蓄積プログラムを格納した記憶媒体であって、

システム内で一意性を持つセッション情報を生成するセッション情報生成プロセスと、

セッション情報を第4の記憶手段に格納すると共に抽出を行うための第4の格納プロセスとを有する。

【0024】

上記のように、本発明によれば、データ及び当該データに対応する署名を格納し、データと1対1に対応する情報であるマニフェストを格納し、署名の生成者である署名者を特定し、マニフェストを格納しようとする者が署名者と同一であるかどうかを検証することにより、署名者の意図した数のマニフェストがデータ蓄積システム内に格納される。

【0025】

また、耐タンバ装置を用いることにより、データをデータ蓄積システム以外に格納することが可能となる。

また、データに対応するマニフェストがデータ蓄積システムに格納されている時のみ、当該データが有効であると区別することにより、マニフェストの数を越えて有効なデータが存在することを防止する。

【0026】

また、データの署名者が信用する署名者である信任対象を指定し、マニフェストに、データ蓄積システムを署名者とする署名を付与し、マニフェストの署名者が信任対象または、信任対象がさらに信用する署名者に含まれること、及び信任情報の署名者と、データの署名者とが同一であることを検証する。これにより、当該データの署名者が信用する経路のみを介してマニフェストを移送することが可能となる。

## 【0027】

さらに、このとき、耐タンパ装置を利用することにより、耐タンパ性が保証される。

また、システム内で一意性を持つセッション情報を生成し、セッション情報を格納することにより、暗号化された通信路を介することなく、1つのマニフェストが複数の格納部に格納されることを防止することが可能となると共に、複数のマニフェストを1つの格納部に並行に転送することが可能となる。

## 【0028】

## 【発明の実施の形態】

図3は、本発明のデータ蓄積システムの全体構成を示す。同図では、権利を表象する電子情報である電子チケットをデータとして発行者が利用者に発行し、チケットを発行された利用者が別の利用者間に譲渡し、チケット譲渡された利用者がチケットを消費する際に、検証者がチケットの有効性を検証する場合を示している。

## 【0029】

同図において、チケットの発行者は、発行者装置1を有し、チケットの発行先となる利用者は利用者装置2を有している。チケットの発行の際には、発行者装置1と利用者2の間は、接続装置4を介して通信手段が確立される。この通信手段は、発行の開始から終了までの間のみ確立されていればよい。

また、チケット譲渡の際には、発行時と同様に利用者装置2間で接続装置4を介して通信手段を確立し、チケットを利用者装置2間で転送する。チケットの改札者は、改札者装置3を有している。チケット改札の際には、発行時と同様に、利用者装置2と改札者装置3との間で接続装置4を介して、通信手段を確立し、改札者装置3にチケットを転送する。

## 【0030】

チケット改札者は、改札者装置3を有している。チケットの改札の際には、発行時と同様に利用者装置2と改札者装置3との間で接続装置4を介して通信手段を確立し、改札者装置3にチケットを転送する。

このように、本発明にかかるデータ蓄積システムは、一時的な相互通信手段を



提供する接続装置 4 により接続された、1 乃至複数の発行者装置 1 と、1 乃至複数の利用者装置 2 と、1 乃至複数の改札者装置 3 とから構成されるシステムである。

【0031】

【実施例】

以下、図面と共に本発明の実施例を説明する。

ここで、図 4 から図 7 を用いて、上記データ蓄積システムを構成する各装置について説明する。以下に、説明で用いる式の意味を示す。

$x \parallel y$  とは、 $x$  と  $y$  の連接である。

【0032】

$H$  とは、一方向のハッシュ関数であり、 $y = H(x)$  を満たすような  $x$  を  $y$  から求めることが困難であるという性質を持つ。このようなハッシュ関数として、米 RSA 社の MD5 などが知られている。

$S_{pk}$  とは、検証関数  $V_{pk}$  により検証可能な電子署名を生成する署名関数である。

。

【0033】

$V_{pk}$  は、検証関数であり、 $V_{pk}(x \parallel S_{pk}(x)) = 1$ 、 $V_{pk}(\text{other}) = 0$  という性質を持つ。即ち、ある情報  $x$  が署名関数  $S_{pk}$  により署名されたものであるかどうかを検証できる性質を持つ。

$P_k$  は、検証鍵であり、検証器  $V$  に検証鍵  $P_k$  を与えることにより、 $V_{pk}$  を構成することが可能であるという性質を持つ。署名が付与された検証鍵  $P_{k2} \parallel S_{pk1}(P_{k2})$  を特に、 $P_{k1}$  による  $P_{k2}$  の鍵証明書と呼ぶ。

【0034】

以上で述べたような性質を持つ  $S_{pk}$ 、 $V_{pk}$  を実現するような電子署名方式として、日本電信電話の E S I G N などが知られている。

図 4 は、本発明の一実施例の発行者装置の構成を示す。

同図に示す発行者装置 1 は、制御部 11、署名部 12、データ生成部 13、マニフェスト生成部 14、信任情報生成部 15 から構成される。

【0035】

制御部 11 は、検証鍵  $P_{kI}$  を保持し、チケットの流通を安全に行うための制御を行う。ここで、 $P_{kI}$  は後述する署名部 12 が備える署名関数  $S_{PkI}$  に対応する検証鍵である。制御部 11 による制御の詳細については後述する。

署名部 12 は、署名関数  $S_{PkI}$  を備える。署名関数  $S_{PkI}$  は、発行者装置 1 毎にそれぞれ異なり、署名部 12 により秘匿される。

【0036】

データ生成部 13 は、内部で生成した情報に基づいて、もしくは、外部から与えられた情報に基づいて、データ  $m$  を生成する。本発明に係るデータ蓄積システムでは、データ  $m$  の記述内容についてなんら制限を持つものではないため、データ  $m$  として切符やコンサートチケットなどの一般的なチケットによって扱われる権利を表象する電子情報の他、プログラム、音楽、画像データなどを扱うことが可能である。

【0037】

マニフェスト生成部 14 は、一方向のハッシュ関数  $H$  を備え、署名付きデータ  $m \parallel S_{PkI}(m)$  のマニフェスト  $c_{(m, PkI)} = H(m \parallel S_{PkI}(m))$  を生成する。

信頼情報生成部 15 は、信頼情報  $t = (t_I, t_C)$  を生成する。 $(t_I, t_C)$  は、それぞれ以下のように構成される。

$$t_I = P_{kI}$$

$$t_C = \{H(P_{kC_1}), H(P_{kC_2}), \dots, H(P_{kC_n})\}$$

ここで、 $P_{kI}$  は、制御部 11 が保持する検証鍵、 $P_{kC_i}$  は発行者が「信用する」第三者（後述）による署名を検証するための検証鍵である。

【0038】

図 5 は、本発明の一実施例の利用者装置の構成を示す。同図に示す利用者装置 2 は、制御部 21、格納部 22 と、制御部 23、認証部 24、署名部 25、番号生成部 26、格納部 27 から構成する耐タンパ装置 28 を有する。各部の機能や内容が改竄されることを（利用者本人からも）防止する。このような耐タンパ装置 28 として、IC カードや、ネットワーク経由で構成され、第三者により厳重に管理されたサーバなどが利用可能である。

【0039】

制御部 21 は、耐タンパ装置 28 に封入された制御部 26 と共に、チケットの流通を安全に行うための制御を行う。制御部 21 による制御の詳細については後述する。

格納部 22 は、利用者が保持する署名付きデータの集合  $M_U$  及び発行者による署名付きの信頼情報の集合  $T_U$  を格納する。これらの集合は、制御部 21 により更新可能である。

#### 【0040】

制御部 23 は、検証鍵  $P_{kU}$ 、 $P_{kC}$  及び鍵証明書  $P_{kU} \parallel S_{PkC}$  ( $P_{kU}$ ) を保持し、制御部 21 と共に、チケットの流通を安全に行うための制御を行う。ここで  $P_{kU}$  は署名部 25 が備える  $S_{PkU}$  に対応する検証鍵であり、 $S_{PkC}$  は、IC カード製造者もしくは、耐タンパサーバ管理者など、耐タンパ装置 28 の安全性を保証する第三者により秘匿される署名関数である。即ち、署名関数  $S_{PkU}$  を含む耐タンパ装置 28 は、署名関数  $S_{PkC}$  を保有する第三者により耐タンパ性が保証されている。制御部 23 による制御の詳細については後述する。また、 $P_{kC}$  は、 $S_{PkC}$  の検証鍵である。

#### 【0041】

認証部 24 は、検証器  $V$  を備える。

署名部 25 は、署名関数  $S_{PkU}$  を備える。 $S_{PkU}$  は、利用者装置 2 毎にそれぞれ異なり、署名部 25 により秘匿される。

番号生成部 26 は、次番号  $r_U$  を保持し、番号の払出しを要求されると、現在の番号  $r_U$  の値を返却すると共に、 $r_U$  をインクリメントする。

#### 【0042】

格納部 27 は、マニフェストの集合  $C_U = \{c_1, c_2, \dots, c_n\}$  及び番号の集合  $R_U = \{r_1, r_2, \dots, r_m\}$  を格納する。これらの集合は、制御部 21 により更新可能である。

図 6 は、本発明の一実施例の改札者装置の構成を示す。

同図に示す改札者装置 3 は、制御部 31、認証部 32、番号生成部 33、及び格納部 34 から構成される。

#### 【0043】

制御部 31 は、検証鍵  $Pk_V$  を備え、チケットの流通を安全に行うための制御を行う。制御部 31 による制御の詳細については後述する。

認証部 32 は、検証器  $V$  を備える。

番号生成部 33 は、次番号  $r_v$  を保持し、番号の払出しを要求されると、 $r_v$  を返却すると共に、 $r_v$  をインクリメントする。

#### 【0044】

格納部 34 は、番号の集合  $R_v = \{r_1, r_2, \dots, r_m\}$  を格納する。これらの集合は、制御部 31 により更新可能である。

図 7 は、本発明の一実施例の接続装置 4 の構成を示す。

同図に示す接続装置 4 は、通信部 41 を有する。通信部 41 は、発行者装置 1、利用者装置 2、改札者装置 3 間や利用者装置 2 相互間での一時的もしくは、永続的な通信手段を提供する。ここで、接続装置 4 として IC カード挿入口を備えたキオスク端末や、ネットワークを介して相互接続された複数の PC などが利用可能である。

#### 【0045】

上述したような構成を有する各装置を用いて、電子チケットの流通を安全に行う方式を以下において説明する。

以下で述べる流通方式における基本的な考え方は、以下のようなものである。

- ・チケット本体は、発行者による署名付きのデータ  $m \parallel S_{PkI}(m)$  で表現されるものとする。 $m$  には、発行者がチケットの所有者に与える権利の内容が記述されているものとする。

#### 【0046】

- ・チケット発行者の署名  $S_{PkI}$  により、チケットの改竄は防止できる。
- ・チケット本体の複製は、特に禁止しない。
- ・チケット本体から、そのチケットに対応するマニフェスト  $c(m, PkI)$  を生成できる。このマニフェストは、事実上チケットに 1 対 1 に対応する。
- ・マニフェストは、発行者が信用できる耐タンパ装置 28 内の格納部 27 に格納されることにより、「有効」なものとなる。

#### 【0047】

・発行者が信用できる耐タンパ装置とは、発行者が信用する者によって耐タンパ性が保証された装置である。発行者が信用する者は、信頼情報  $t_I$  により規定される。

・チケットを消費もしくは、譲渡するためには、有効なマニフェストが必要である。

【0048】

・有効なマニフェストは、対応するチケットの発行者のみが新規に作成可能である。

・1つの有効なマニフェストから、複数の有効なマニフェストを作成することを禁止する。即ち、利用者が勝手に有効なマニフェストを作成することを不可能にする。

【0049】

以下、(1) チケット発行の場合、(2) チケット譲渡の場合、(3) チケット検証の場合、のそれぞれの場合に分けてチケットの流通方式を説明する。なお、各装置を跨がるそれぞれの通信は、接続装置4中の通信部41を介するものとする。

(1) チケット発行の場合：

以下は、発行者装置1から利用者装置2に対する接続装置4を介したチケット発行処理の流れである。

【0050】

図8は、本発明の一実施例のチケット発行処理のシーケンスチャートである。

ステップ101) 制御部11は、以下の手順により  $m$  及び  $S_{pkI}(m)$  を得て、署名付きデータであるところのチケット  $m \parallel S_{pkI}(m)$  の生成を行う。

(a) データ生成部13によりデータ  $m$  を生成する。

(b) 署名部12に  $m$  を与え、 $S_{pkI}(m)$  を生成する。

【0051】

ステップ102) 制御部11は、マニフェスト生成部14にチケット  $m \parallel S_{pkI}(m)$  を与え、マニフェスト  $c(m, pkI)$  を生成する。

ステップ103) 制御部11は、以下の手順により信頼情報  $t$  及び署名関数

$S_{pkI}(t)$  を得て、署名付き信頼情報  $t \parallel S_{pkI}(t)$  の生成を行う。

(a) 信頼情報生成部 15 により、信頼情報  $t$  を生成する。 $t$  の構成は、前述の通りである。

【0052】

(b) 署名部 12 に信頼情報  $t$  を与え、署名  $S_{pkI}(t)$  を生成する。

ステップ 104) 制御部 11 は、制御部 21 にチケット  $m \parallel S_{pkI}(m)$  と署名付き信頼情報  $t \parallel S_{pkI}(t)$  を転送する。

ステップ 105) 制御部 21 は、チケット  $m \parallel S_{pkI}(m)$  を格納部 22 の  $M_U$  に、署名付き信頼情報  $t \parallel S_{pkI}(t)$  を格納部 22 の信頼情報の集合  $T_U$  にそれぞれ追加して格納する。

【0053】

ステップ 106) 制御部 21 は、制御部 23 にセッション情報  $(s_1, s_2)$  の生成を依頼する。

制御部 23 は、以下の手順により、セッション情報  $(s_1, s_2)$  を生成し、制御部 21 に転送する。

(a) 番号生成部 26 により、番号  $r_U$  の払い出しを受ける。

【0054】

(b)  $r_U$  を格納部 27 の番号集合  $R_U$  に追加する。

(c)  $(s_1, s_2) = (H(PkU), r_U)$  を生成する。ここで、 $PkU$  は、制御部 21 が保持する検証鍵である。

ステップ 107) 制御部 21 は、制御部 11 にセッション情報  $(s_1, s_2)$  を転送する。

【0055】

ステップ 108) 制御部 11 は、署名部 12 が備える  $S_{pkI}$  と制御部 11 が保持する検証鍵  $PkI$  を用い、マニフェスト発行形式  $e_I = (e_1, e_2, e_3, e_4, e_5)$  を得る。ここで、 $e_I$  の各要素は以下の値をとる。

$$e_1 = c(m, PkI),$$

$$e_2 = s_1$$

$$e_3 = s_2$$

$$e_4 = S_{PkI} (c_{(m,PkI)} \parallel s_1 \parallel s_2)$$

$$e_5 = PkI$$

ステップ109) 制御部11は、制御部21にマニフェスト発行形式 $e_I$ を転送する。

【0056】

ステップ110) 制御部21は、制御部23にマニフェスト発行形式 $e_I$ を転送し、 $e_I$ 内のマニフェストの格納を依頼する。

ステップ111) 制御部23は、認証部24を用い、以下の式で全てが成立することを検証する。検証に失敗した場合、以後の処理を中断し、制御部21を介して、制御部11に処理の中断の通知を行う。

【0057】

$$e_2 = H(PkU) \quad (1)$$

$$e_3 \in R_U \quad (2)$$

$$V_{e5}(m \parallel S_{PkI}(m)) = 1 \quad (3)$$

$$V_{e5}(e_1 \parallel e_2 \parallel e_3 \parallel e_4) = 1 \quad (4)$$

上記の式(1)及び式(2)は、セッション情報の正当性の検証である。この検証により、他の利用者装置2宛のマニフェスト発行形式を格納すること、及びマニフェスト発行形式の再利用によってマニフェストを複製すること、などの不正を防止する。式(3)及び式(4)は、マニフェスト発行形式に対する署名の正当性の検証である。この検証により、チケットの発行者が署名したマニフェスト発行形式に含まれるマニフェスト以外を格納することを防止する。

【0058】

ステップ112) 制御部23は、格納部27の番号集合 $R_U$ から $e_3 (= r_U)$ を削除する。

ステップ113) 制御部23は、格納部27のマニフェストの集合 $C_U$ に $e_1 (= c_{(m,PkI)})$ を追加する。

ステップ114) 制御部23は、制御部21に $e_1$ を転送し、処理の正常終了を通知する。

【0059】

ステップ 115) 制御部 21 は、以下の式が成立することを検証する。検証に失敗した場合は、処理の中断を、検証に成功した場合は、処理の正常終了を、制御部 11 に通知する。

$$H(m \parallel S_{pkI}(m)) \in C_U \quad (5)$$

上記の式 (5) は、発行されたチケットに対応するマニフェストが格納部 27 に格納されたことの検証である。この検証により、有効なマニフェストが合わせて発行されたこと、即ち、発行されたチケットが有効であることを確認する。

#### 【0060】

(2) チケット譲渡の場合：

以下は、利用者装置 2a から利用者装置 2b に対する接続装置 4 を介したチケット譲渡処理の流れである。

図 9、図 10 は、本発明の一実施例のチケット譲渡処理のシーケンスチャートである。

#### 【0061】

ステップ 201) 制御部 21a は、格納部 22a が保持する署名付きデータの集合  $M_{Ua}$  から譲渡対象となるチケット  $m \parallel S_{pkI}(m)$  を抽出する。

ステップ 202) 制御部 21a は、格納部 22a が保持する  $T_{Ua}$  から  $m \parallel S_{pkI}(m)$  の発行者による署名付き信頼情報  $t \parallel S_{pkI}(t)$  を抽出する。

ステップ 203) 制御部 21a は、制御部 21b に  $m \parallel S_{pkI}(m)$  と  $t \parallel S_{pkI}(t)$  を転送する。

#### 【0062】

ステップ 204) 制御部 21b は、 $m \parallel S_{pkI}(m)$  を格納部 22b の署名付きデータの集合  $M_{Ub}$  に、 $t \parallel S_{pkI}(t)$  を格納部 22 の信頼情報の集合  $T_{Ub}$  に、それぞれ格納する。

ステップ 205) 制御部 21b は、制御部 23b にセッション情報 ( $s_1$ ,  $s_2$ ) の生成を依頼する。制御部 23b は、以下の手順により ( $s_1$ ,  $s_2$ ) を生成し、制御部 21b に転送する。

#### 【0063】

(a) 番号生成部 26b により番号  $r_{Ub}$  の払出しを受ける。



(b)  $r_{Ub}$  を格納部 27b の番号集合  $R_{Ub}$  に追加する。

(c)  $(s_1, s_2) = (H(PkUb), r_{Ub})$  を生成する。ここで、 $PkUb$  は、制御部 21b が保持する検証鍵である。

ステップ 206) 制御部 21b は、制御部 21a に  $(s_1, s_2)$  を転送する。

【0064】

ステップ 207) 制御部 21a は、制御部 23a に  $(s_1, s_2)$  と譲渡対象チケットのハッシュ  $H(m \parallel S_{PkI}(m))$  を転送する。

ステップ 208) 制御部 23a は、格納部 27a に格納されたマニフェスト集合  $C_{Ua}$  について、以下の式が成立することを検証する。検証に失敗した場合、以後の処理を中断し、制御部 21a に処理の失敗を通知する。

【0065】

$$H(m \parallel S_{PkI}(m)) \in C_{Ua} \quad (6)$$

上記の式 (6) は、譲渡対象チケットに対応するマニフェスト  $c_{(m,PkI)} = H(m \parallel S_{PkI}(m))$  が格納部 27a に格納されていることの検証である。

ステップ 209) 制御部 23a は、署名部 25a が備える  $S_{PkUa}$  と制御部 11 が保持する検証鍵  $PkUa$ 、 $PkCa$  及び鍵証明書  $PkUa \parallel S_{PkCa}(PkUa)$  を用い、マニフェスト転送形式  $e_c = (e_1, e_2, e_3, e_4, e_5, e_6, e_7)$  を得る。ここで、 $e_c$  の各要素は、以下の値となる。

【0066】

$$e_1 = c_{(m,PkI)}$$

$$e_2 = s_1$$

$$e_3 = s_2$$

$$e_4 = S_{PkUa}(c_{(m,PkI)} \parallel s_1 \parallel s_2)$$

$$e_5 = PkUa$$

$$e_6 = S_{PkCa}(PkUa)$$

$$e_7 = PkCa$$

ステップ 210) 制御部 23a は、マニフェスト集合  $C_{Ua}$  から  $c_{(m,PkI)}$  を削除する。

## 【0067】

ステップ211) 制御部23aは、制御部21aに $e_C$ を転送する。

ステップ212) 制御部21aは、制御部21bに $e_C$ を転送する。

ステップ213) 制御部21bは、制御部23bに $e_C$ ， $t \parallel S_{PkI}(t)$ ， $m \parallel S_{PkI}(m)$ を転送し、 $e_C$ 内のマニフェストの格納を依頼する。

ステップ214) 制御部23bは、認証部24bを用い、以下の式で全てが成立することを検証する。検証に失敗した場合、以後の処理を中断し、制御部21bに処理の中断を通知する。

## 【0068】

$$e_2 = H(PkUb) \quad (7)$$

$$e_3 \in R_{Ub} \quad (8)$$

$$V_{ea}(e_1 \parallel e_2 \parallel e_3 \parallel e_4) = 1 \quad (9)$$

$$V_{er}(e_5 \parallel e_6) = 1 \quad (10)$$

$$H_{(er)} \in t_c \quad (11)$$

$$V_{t1}(m \parallel S_{PkI}(m)) = 1 \quad (12)$$

$$V_{t1}(t \parallel S_{PkI}(t)) = 1 \quad (13)$$

上記の式(7)及び式(8)は、セクション情報の正当性の検証である。この検証により、他の利用者装置2宛のマニフェスト転送形式を格納すること、及びマニフェスト転送形式の再利用により、マニフェストを複製すること、などの不正を防止する。

## 【0069】

式(9)は、マニフェスト転送形式の署名者を特定するための検証であり、式(10)は、該署名者の鍵証明書を検証であり、式(11)は、当該鍵証明書の書名者が、信頼情報中の信頼情報中の信頼対象として発行者により信任されていることの検証である。これらの検証により、発行者が信用する者によって当該マニフェスト転送形式の転送元の耐タンパ性が保証されていることを確認する。

## 【0070】

式(12)及び式(13)は、当該信頼情報に対する署名の正当性の検証である。この検証により、当該信頼情報が当該チケットの署名者により正しく署名さ

れていることを確認する。

ステップ 2 1 5) 制御部 2 3 b は、格納部 2 7 b の番号の集合  $R_{Ub}$  から  $e_3$  ( $= r_{Ub}$ ) を削除する。

【0 0 7 1】

ステップ 2 1 6) 制御部 2 3 b は、格納部 2 7 b のマニフェスト集合  $C_{Ub}$  に  $e_1$  ( $= c_{(m, PkI)}$ ) を追加する。

ステップ 2 1 7) 制御部 2 3 b は、制御部 2 1 b に処理の正常終了を通知する。

ステップ 2 1 8) 制御部 2 1 b は、以下の式が成立することを検証する。検証に失敗した場合は、処理の中断を、検証に成功した場合は、処理の正常終了を、制御部 2 1 a に通知する。

【0 0 7 2】

$$H(m \parallel S_{PkI}(m)) \in C_{Ub} \quad (14)$$

上記の式 (14) は、譲渡されたチケットに対応するマニフェストが格納部 2 7 b に格納されたことの検証である。この検証により、有効なマニフェストが合わせて転送されたこと、即ち、譲渡されたチケットが有効であることを確認する。

【0 0 7 3】

(3) チケット消費の場合：

以下は、利用者装置 2 から改札者装置 3 に対する、接続装置 4 を介したチケット消費処理の流れである。

図 1 1 は、本発明の一実施例のチケット消費のシーケンスチャートである。

ステップ 3 0 1) 制御部 2 1 は、格納部 2 2 が保持する署名付きデータの集合  $M_U$  から消費対象となるチケット  $m \parallel S_{PkI}(m)$  を抽出する。

【0 0 7 4】

ステップ 3 0 2) 制御部 2 1 は、格納部 2 2 が保持する署名付き信頼情報の集合  $T_U$  から  $m \parallel S_{PkI}(m)$  の発行者による署名付き信頼情報  $t \parallel S_{PkI}(t)$  を抽出する。

ステップ 3 0 3) 制御部 2 1 は、制御部 3 1 に  $m \parallel S_{PkI}(m)$  と  $t \parallel S_{PkI}(t)$  を送信する。

$I(t)$  を転送する。

【0075】

ステップ304) 制御部31は、以下の手順によりセッション情報  $(s_1, s_2)$  を生成する。

(a) 番号生成部33により番号  $r_v$  の払出しを受ける。

(b)  $r_v$  を格納部34の番号集合  $R_v$  に追加する。

(c)  $(s_1, s_2) = (H(PkV), r_v)$  を生成する。 $PkV$ は制御部31が保持する検証鍵である。

【0076】

ステップ305) 制御部31は、制御部21にセッション情報  $(s_1, s_2)$  を転送する。

ステップ306) 制御部21は、制御部23に、 $(s_1, s_2)$  と消費対象チケットのハッシュ  $H(m \parallel S_{PkI}(m))$  を転送する。

ステップ307) 制御部23は、格納部27に格納されたマニフェスト集合  $C_U$  について、以下の式が成立することを検証する。検証に失敗した場合には、以後の処理を中断し、制御部21に処理の失敗を通知する。

【0077】

$$H(m \parallel S_{PkI}(m)) \in C_U \quad (15)$$

上記の式(15)は、消費対象チケットに対応するマニフェスト  $c_{(m, PkI)} = H(m \parallel S_{PkI}(m))$  が格納部27に格納されていることの検証である。

ステップ308) 制御部23は、署名部25が備える署名関数  $S_{PkU}$  と制御部11が保持する検証鍵  $PkU$ ,  $PkC$  及び鍵証明書  $PkU \parallel S_{PkC}(PkU)$  を用い、マニフェスト転送形式  $e_C = (e_1, e_2, e_3, e_4, e_5, e_6, e_7)$  を得る。ここで、 $e_C$  の各要素は以下の値をとる。

【0078】

$$e_1 = c_{(m, PkI)}$$

$$e_2 = s_1$$

$$e_3 = s_2$$

$$e_4 = S_{PkU}(c_{(m, PkI)} \parallel s_1 \parallel s_2)$$

$$e_5 = P k U$$

$$e_6 = S_{pkC} (P k U)$$

$$e_7 = P k C$$

ステップ 309) 制御部 23 は、マニフェスト集合  $C_U$  から  $c_{(m, PkI)}$  を削除する。

【0079】

ステップ 310) 制御部 23 は、制御部 21 に  $e_C$  を転送する。

ステップ 311) 制御部 21 は、制御部 31 に  $e_C$  を転送する。

ステップ 312) 制御部 31 は、認証部 32 を用い、以下の式の全てが成立することを検証する。検証に失敗した場合、以後の処理を中断し、制御部 21 に処理の中断を通知する。

【0080】

$$e_2 = H (P k V) \quad (16)$$

$$e_3 \in R_V \quad (17)$$

$$V_{cb} (e_1 \parallel e_2 \parallel e_3 \parallel e_4) = 1 \quad (18)$$

$$V_{e7} (e_5 \parallel e_6) = 1 \quad (19)$$

$$H (e_r) \in t_C \quad (20)$$

$$V_{tI} (m \parallel S_{pkI} (m)) = 1 \quad (21)$$

$$V_{tI} (t \parallel S_{pkI} (t)) = 1 \quad (22)$$

上記の式 (16) 及び式 (17) は、セッション情報の正当性の検証である。この検証により、他の改札者装置 3 宛のマニフェスト転送形式を格納すること、及び自分宛のマニフェスト転送形式の再利用により、マニフェストを複製すること、などの不正を防止する。

【0081】

式 (18) は、マニフェスト転送形式の署名者を特定するための検証であり、式 (19) は、当該署名者の鍵証明書を検証であり、式 (20) は、当該鍵証明書の署名者が信頼情報中の信頼対象として発行者により信任されていることの検証である。これらの検証により、発行者が信用する者によって当該マニフェスト転送形式の転送元の耐タンパ性が保証されていることを確認する。

## 【0082】

式(21)及び式(22)は、当該信任情報に対する署名の正当性の検証である。この検証により、当該信任情報が当該チケットの署名者により正しく署名されていることを確認する。

ステップ313) 制御部31は、格納部34の $R_V$ から $e_3 (= r_V)$ を削除する。

## 【0083】

ステップ314) 制御部31は、以下の式が成立することを検証する。検証に失敗した場合は、処理の中断を制御部21に通知する。検証に成功した場合は、 $m$ に対応するサービスを消費者に提供する。

$$e_1 = H(m \parallel S_{pkI}(m)) \quad (23)$$

上記の式(23)は、消費されたチケットに対応するマニフェストが転送されたことの検証である。この検証により、有効なマニフェストが併せて転送されたこと、即ち、有効なチケットが消費されたことを確認する。

## 【0084】

また、前述の図3に示す発行者装置1、利用者装置2、改札装置3の各構成要素をプログラムとして構築し、発行者装置、利用者装置、改札装置として利用されるコンピュータに接続されるディスク装置や、フロッピーディスクやCD-ROM等の可搬記憶媒体に格納しておき、本発明を実施する際に、各コンピュータにインストールすることにより容易に本発明を実現できる。

## 【0085】

なお、本発明は、上記の実施例に限定されることなく、特許請求の範囲内において種々変更・応用が可能である。

## 【0086】

## 【発明の効果】

上述のように、本発明によれば、データの署名者の意図した数だけマニフェストをデータ蓄積システムのマニフェスト格納部に格納し、当該署名者以外が該マニフェストを新たに格納することを防止する、該マニフェストの数を越えて有効なデータが存在することを防止する、当該署名者が信用する経路のみを介してマ

ニフェストを移送することが可能となる。

【0087】

チケットを本発明のデータ蓄積システムのデータとして用いることにより、チケット自体を耐タンパ装置に格納することなしに、チケットの有効な複製数を一定に保つことが可能となる。

また、プログラムを本発明におけるデータとして用い、当該プログラムの実行ライセンスをマニフェストとして用いることにより、不当に複製された当該プログラムの実行を防止することが可能となる。

【0088】

また、音楽データや画像データを本発明におけるデータとして用い、当該データの鑑賞権をマニフェストとして用いることにより、不当に複製された当該データの鑑賞を防止することが可能となる。

さらに、データを鑑賞する毎に当該データを「消費（実施例における（3））」することにより、利用毎の課金システム（pay per view 課金）などに利用することが可能である。

【図面の簡単な説明】

【図1】

本発明の原理を説明するための図である。

【図2】

本発明の原理構成図である。

【図3】

本発明のデータ蓄積システムの全体構成図である。

【図4】

本発明の一実施例の発行者装置の構成図である。

【図5】

本発明の一実施例の利用者装置の構成図である。

【図6】

本発明の一実施例の改札者装置の構成図である。

【図7】

本発明の一実施例の接続装置の構成図である。

【図 8】

本発明の一実施例のチケット発行処理のシーケンスチャートである。

【図 9】

本発明の一実施例のチケット譲渡処理のシーケンスチャート（その 1）である

【図 1 0】

本発明の一実施例のチケット譲渡処理のシーケンスチャート（その 2）である

【図 1 1】

本発明の一実施例のチケット消費処理のシーケンスチャートである。

【符号の説明】

- 1 発行者装置
- 2 利用者装置
- 3 改札者装置
- 4 接続装置
  - 1 1 制御部
  - 1 2 署名部
  - 1 3 データ生成部
  - 1 4 マニフェスト生成部
  - 1 5 信頼情報生成部
- 2 1 制御部
- 2 2 格納部
- 2 3 制御部
- 2 4 認証部
- 2 5 署名部
- 2 6 番号生成部
- 2 7 格納部
- 3 1 制御部



3 2 認証部

3 3 番号生成部

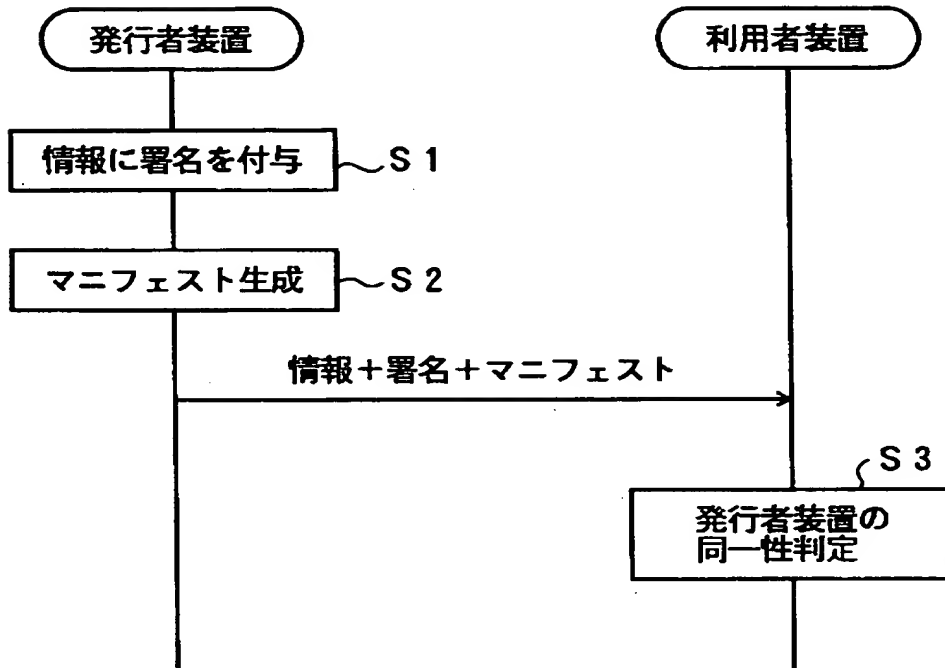
3 4 格納部

4 1 通信部

【書類名】 図面

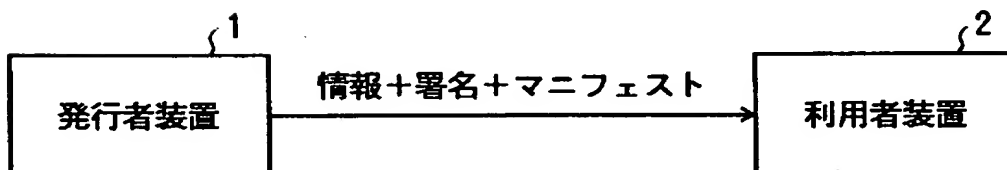
【図 1】

本発明の原理を説明するための図



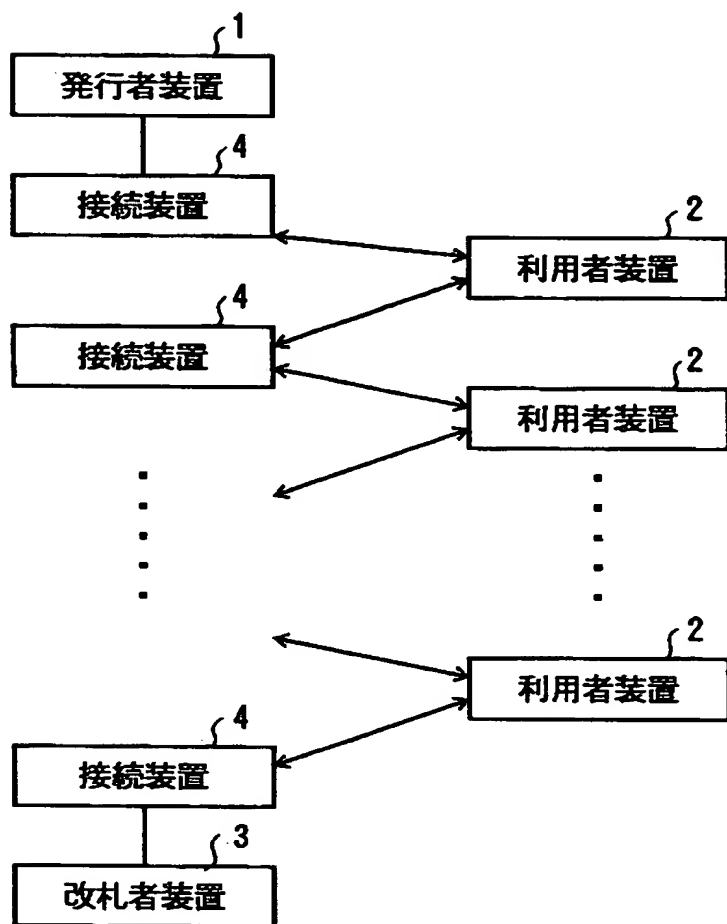
【図 2】

本発明の原理構成図



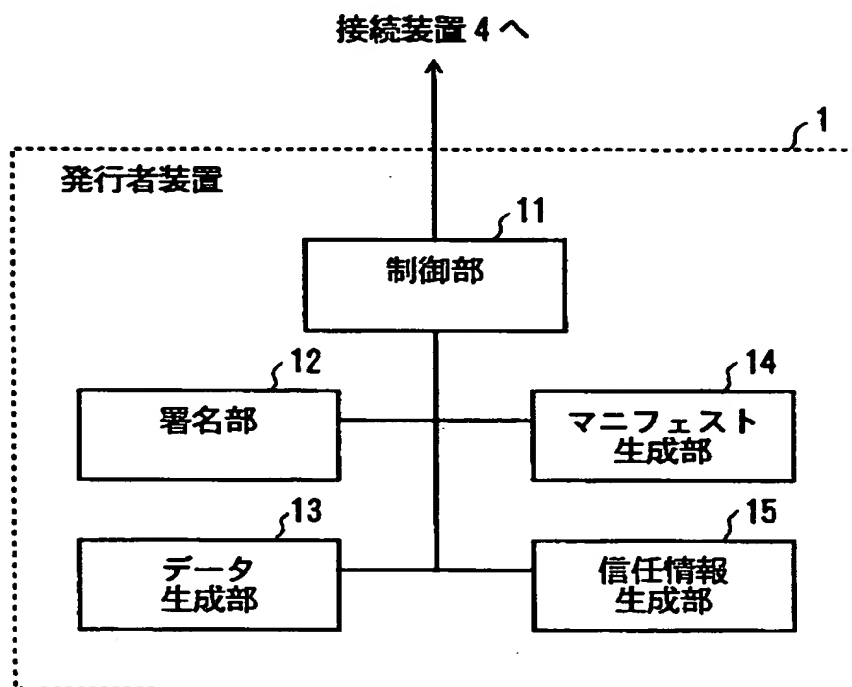
【図 3】

本発明のデータ蓄積システムの全体構成図



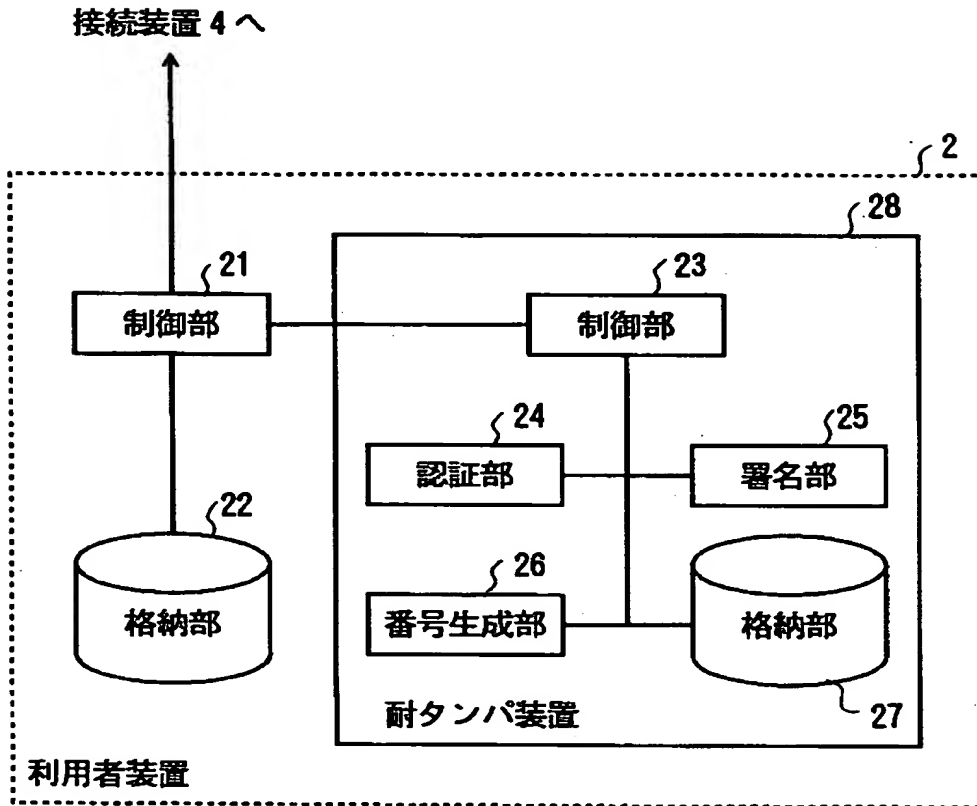
【図 4】

本発明の一実施例の発行者装置の構成図



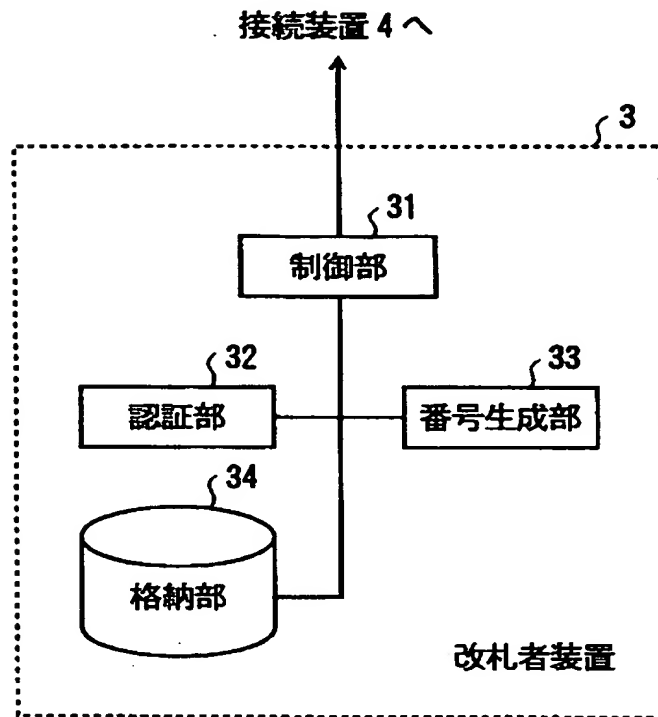
【図 5】

本発明の一実施例の利用者装置の構成図



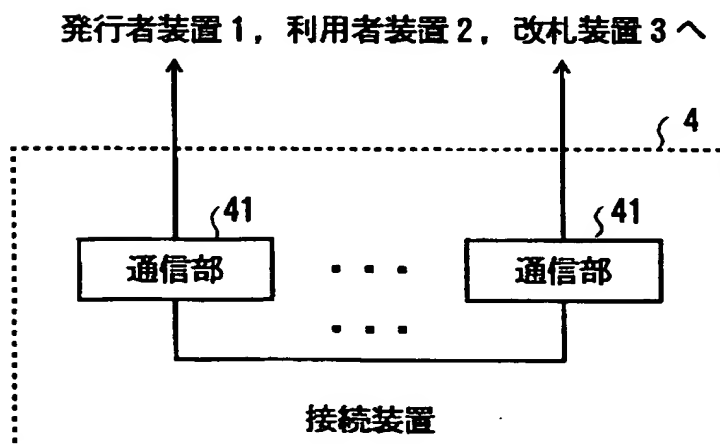
【図 6】

本発明の一実施例の改札者装置の構成図



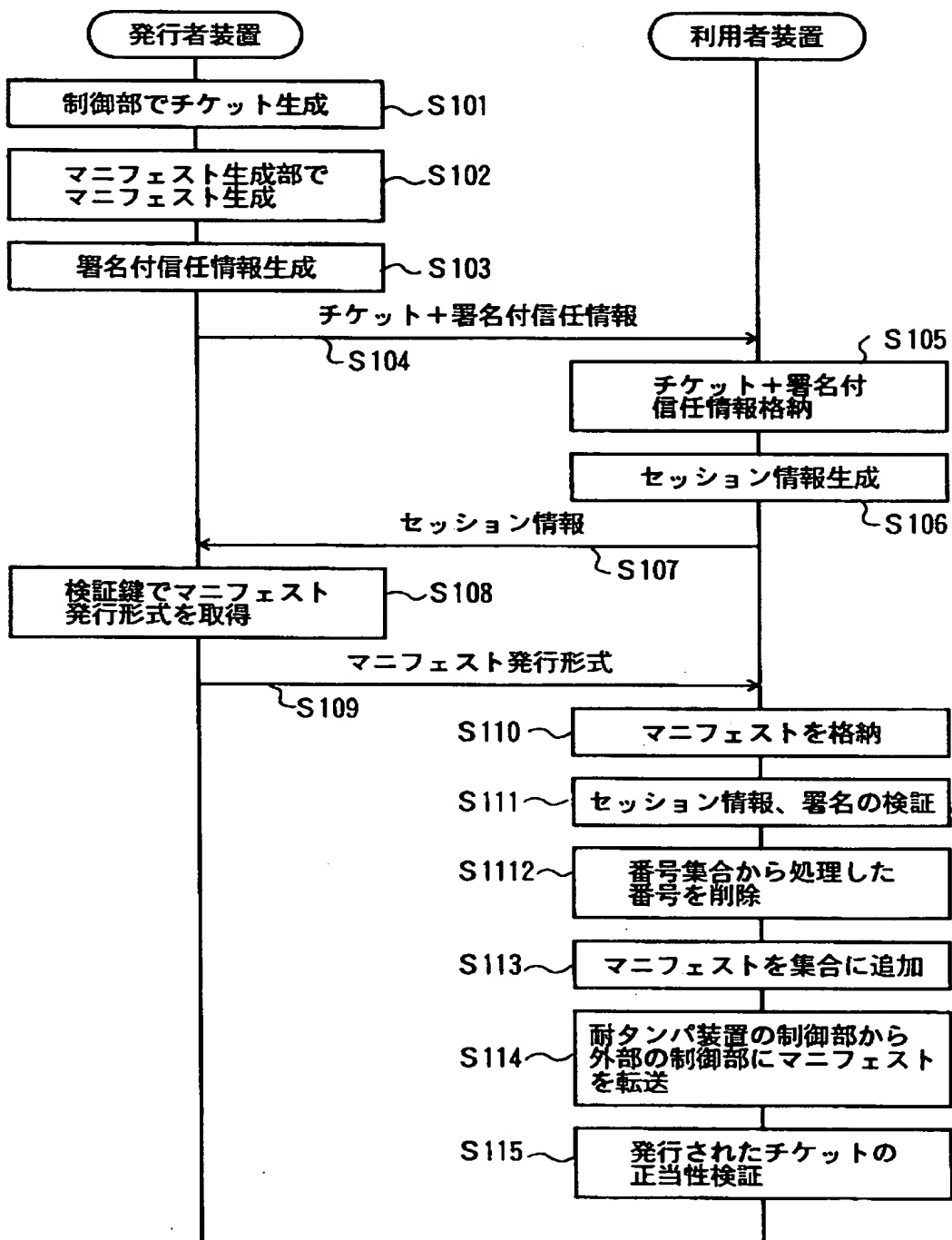
【図 7】

本発明の一実施例の接続装置の構成図



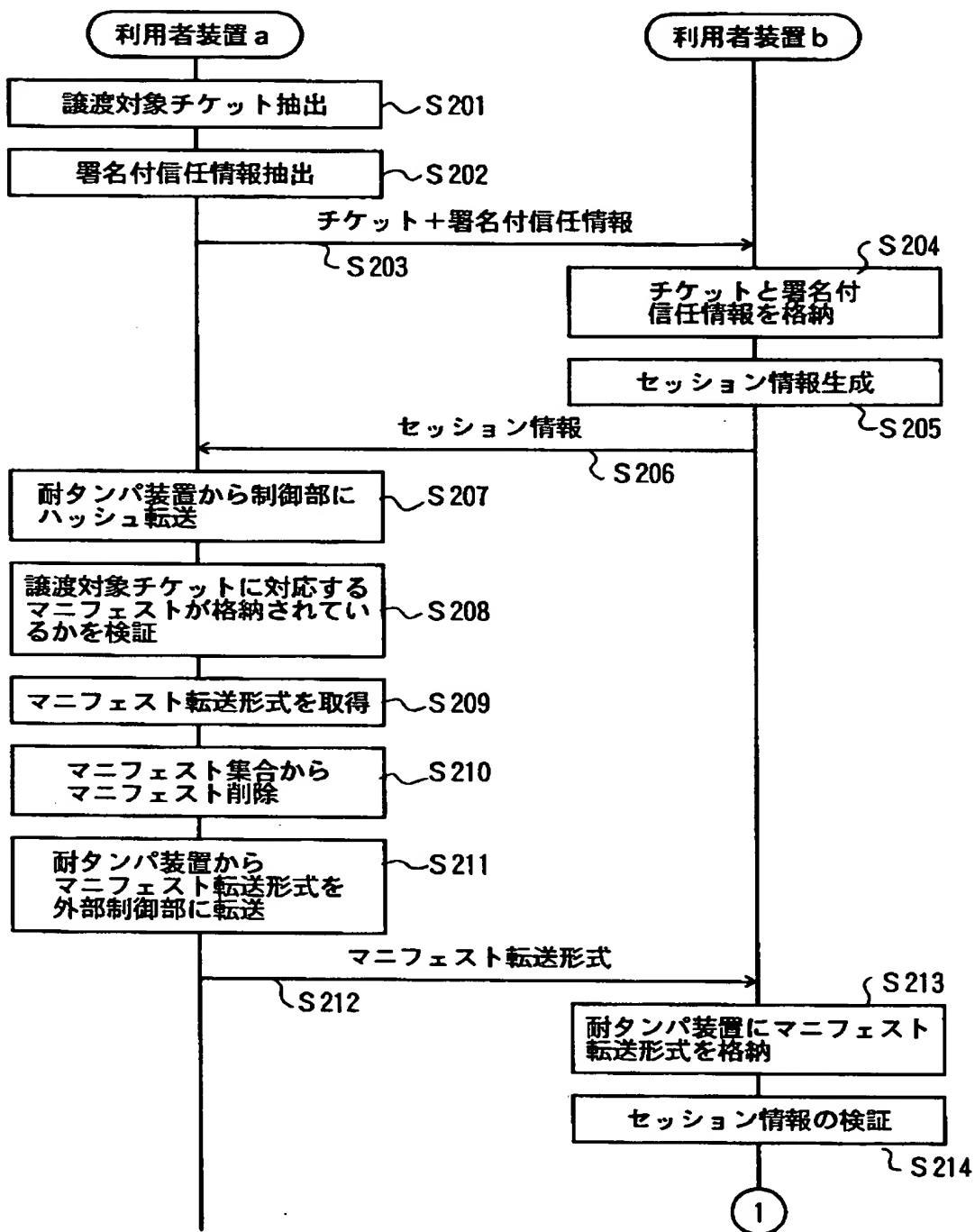
【図 8】

本発明の一実施例のチケット発行処理のシーケンスチャート



【図 9】

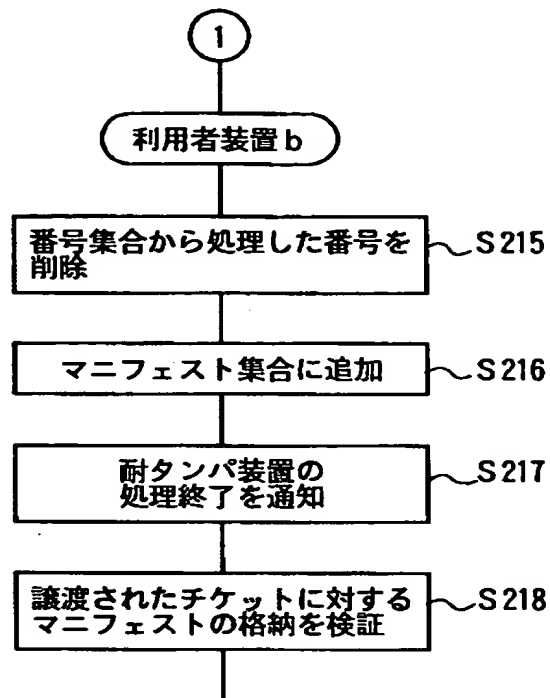
本発明の一実施例のチケット譲渡処理の  
シーケンスチャート（その 1）





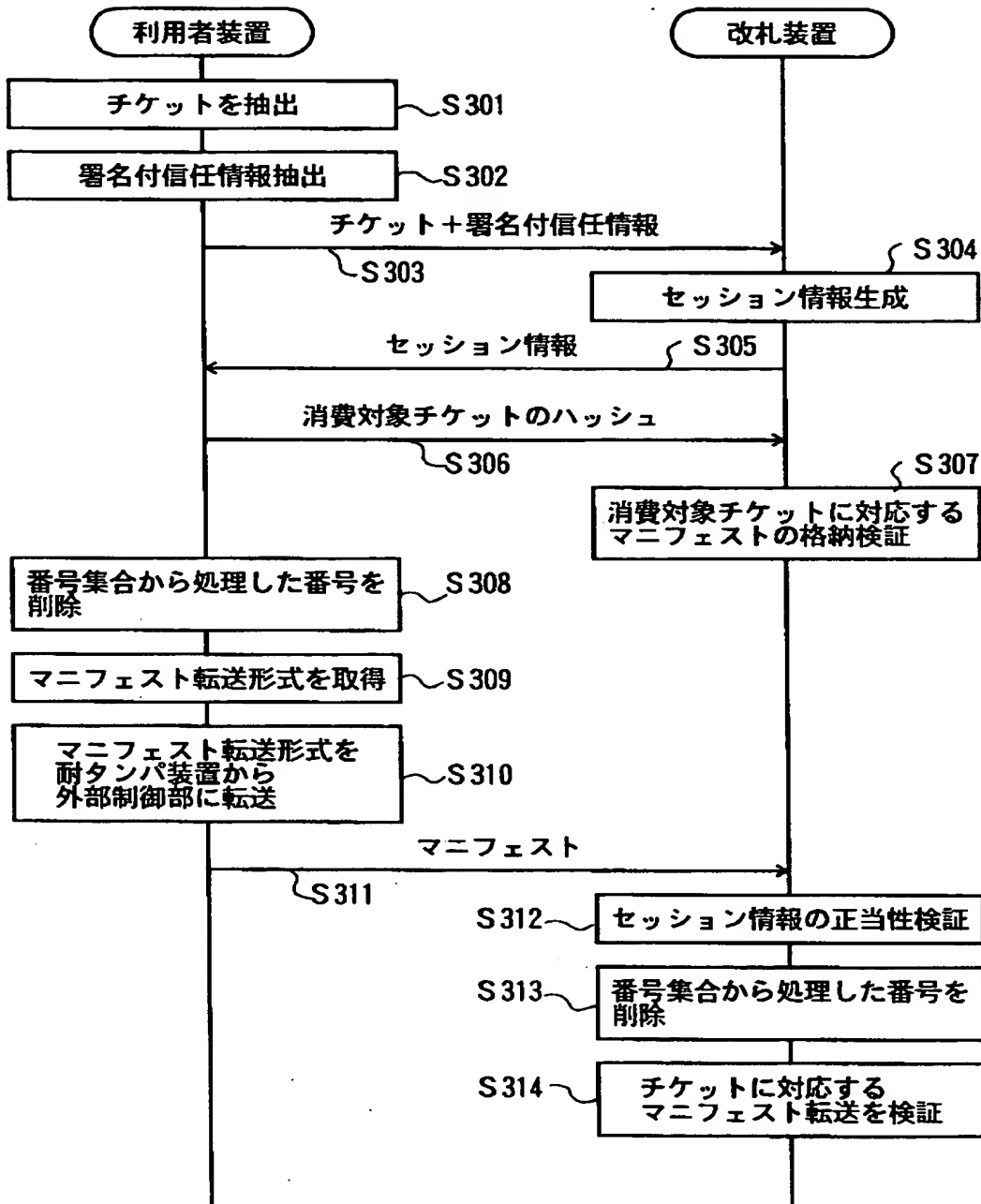
【図 10】

本発明の一実施例のチケット譲渡処理の  
シーケンスチャート（その 2）



【図 11】

本発明の一実施例のチケット消費処理のシーケンスチャート



【書類名】 要約書

【要約】

【課題】 データの有効な複製数を一定以下に保つことを保証しつつ、記述の正当性の検証を含む複製に関する有効性以外の検証をすべて耐タンパ装置に委ねることなく、処理速度や記憶容量等の処理負荷を低減させるデータ蓄積方法及びシステム及びデータ蓄積プログラムを格納した記憶媒体を提供する。

【解決手段】 本発明は、電子的な情報の発行者装置により該電子的な情報に署名した第 1 の情報を付与し、発行者装置により電子的な情報と対応するマニフェストの第 2 の情報を生成して、第 1 の情報に付与し、電子的な情報利用装置において、第 1 の情報と第 2 の情報を用いて電子的な情報の発行者装置の同一性を判定し、電子的な情報の複製を防止する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000004226]

1. 変更年月日 1995年 9月21日  
[変更理由] 住所変更  
住 所 東京都新宿区西新宿三丁目19番2号  
氏 名 日本電信電話株式会社
2. 変更年月日 1999年 7月15日  
[変更理由] 住所変更  
住 所 東京都千代田区大手町二丁目3番1号  
氏 名 日本電信電話株式会社